COMMISSIONER SIMINGTON ADDRESSES PLI
DECEMBER 15, 2022

Hello. Thank you, Barry, for the kind introduction. It is a pleasure to be here.

I am here today to declare that the FCC should take action to solve a serious problem that is putting our wireless networks at risk. Hundreds of millions of devices in active use in this country—more every day, and in more applications—are susceptible to known security vulnerabilities, exposing us to theft of private data and to attacks on the integrity of our public and private networks. But some manufacturers and sellers of these devices plan to do absolutely nothing about it. They don't really care about the ongoing security of devices they sold last year or two years ago, and they've moved on to the new devices they're selling right now. I think they should have to care. They should have the obligation to put out security updates that patch these vulnerabilities. And I hope to convince you today that such a requirement is not only good for the public, but also both good for the technology industry and within the authority of the FCC to implement.

Just last month, we took action to ban untrustworthy equipment from American networks. This was driven in part by concerns that the cameras, routers, and multitudes of other devices across America running software written by Chinese Communist Party controlled companies were inherently a national security risk. Such software could be loaded with intentional backdoors, or plain old accidental vulnerabilities, that hostile governments or hacker syndicates could be the first to know about, and us the last. This foothold in our critical infrastructure could be used to steal our private data, to intentionally cause network disruption, and to set up a mass surveillance web to the benefit of a foreign power. But because of strong Congressional and Commission action culminating in our order last month, we are swiftly and thoroughly rooting out this threat from our networks and making sure it doesn't recur.

What I am proposing today, though, is that we go one step further. It's time to turn our attention to the millions of wireless devices in our country that are insecure, not because they're made by unfriendly state-controlled entities or criminal hackers masquerading as legitimate manufacturers, but rather, because their makers have failed to put sufficient care into making and keeping them secure. Instead of a conspiracy to infiltrate our networks there is an industry-wide acquiescence to careless practices—careless practices that a create the conditions for criminals and other adversaries to hack into our devices, steal our private data, and attack our networks.

Now, there's an outside chance that some device manufacturers are merely cynical about security and your safety, but I don't think that's what's happening. The vast, vast majority of these manufacturers are led by good engineers and thoughtful business leaders fighting to survive in a hyper-competitive market—one of the great strengths of the American electronics industry. They find themselves, however unwillingly, caught in a race to the bottom on price. And in this race to the bottom, engineering for ongoing security throughout the expected lifetime of a device hasn't often made the cut as an essential business expenditure necessary for survival. This is inevitable as devices mature and we come to rely on them more. We expect more safety know-how and tech from auto companies today than we did from Henry Ford. But if the DoT tolerated Model T safety standards today, we'd be outraged.

Reacting to this could easily go wrong. It would be immensely hubristic and naïve to think we can just regulate our way to success, because that would require getting the government to be nimbler than the hackers and better at tech than the tech companies. A market-based approach to safety can leverage the best practices of industry without vainly trying to spell them out every time someone finds a new bug.

I am a Republican and a capitalist. I believe in the free market. I'm also realistic about the limits of the market to produce certain important outcomes. When it comes to products that might cause physical injury, we have long recognized this. The law does not allow you to put a dangerous contraption into the world and then wash your hands of responsibility when people are injured. No, you will be held liable in court. And when serious dangers become apparent, you will be required to issue a recall and take the dangerous device out of the world. The law raises the floor of acceptable engineering and product design and makes it so you can't hope to undercut your competition by skimping on safety, either in manufacture, in design, or in support. A software update is not much different in theory from a recall and retrofit in the world of physical injury causing products. But thankfully for us, it's in practical terms much less burdensome. A physical recall requires identifying and individually contacting every owner of the defective device across the country and either physically moving the product to a repair location or dispatching technicians to every owner's home or place of business. The retrofit almost certainly involves physical labor, and often involves newly manufactured pieces that serve to render the product safer. All of this is extremely expensive, so expensive that courts have long recognized that the decision to mandate a recall is more properly a political and pragmatic one to be made by regulators on a case-by-case basis instead of a principled legal one to be made by courts.

For software updates, especially when a device is furnished with an over-the-air update system to begin with, almost none of this work is required. You don't need to manufacture or move around new physical objects, and you don't need to identify and contact every owner of a device. You don't even need anyone to touch the devices to be updated. In fact, the owners of the devices don't have to be involved at all unless they want heightened control of their networks, the way a large IT department might. All that's required is that the maker identify the flaw in the code, fix it, test it, and release it through their update channels. The burden of releasing a software update—a relatively small amount of labor inside a company's engineering offices—is vastly outweighed by the benefit to society—a dangerous vulnerability being closed on thousands or millions of devices in active use across American households and businesses.

Action is been long overdue. I think most of us in this room remember Microsoft's famous push for a computer on every desk. It wasn't long before wide adoption of the internet networked all of those devices and exposed them to hackers across the country and around the world. Now there's a software-controlled wireless device in every pocket, in every appliance. Dozens in every car. And we're well on our way to wireless computers in every light switch and in every light bulb. And it's not just consumer devices. The factory floor, the flight deck, the utility pole, these are all venues for the mass installation of software-controlled wireless devices. Until now, the FCC's approach to regulating wireless devices has focused on how the device behaves in a testing lab. We take it for granted that the device doesn't have hidden modes, whether intentional or not. And then we mostly forget about it as soon as we issue the

equipment authorization, except to the extent that operators are held to the terms of authorized use, and their spectrum licenses where applicable. Notably, we don't really have anything to say just yet about security vulnerabilities that might turn a device that behaves perfectly well on the test bench into one that spews harmful interference and, for example, takes down every Wi-Fi network in its vicinity.

This was a sensible regime for a long time, when wireless devices either had no software at all or very limited software that was not really susceptible to cyberattacks—definitely not distributed large-scale cyberattacks. No attacker could hope to create botnets—that is, thousands or millions of such devices under their control at the same time—out of old wireless devices, which were not internet connected and not able to run user-defined software. There's no such thing as a botnet of CB radios, remote-control cars, or TV clickers.

But times have changed. The phone in your pocket is now a supercomputer, by some measures 100,000 times as powerful as the guidance computer for the Moon landing, and it ships with more software than a desktop computer did only a few years ago—no wonder, because it likely contains six to twelve radios, all requiring sophisticated software to operate them. And security experts essentially take it for granted that any non-trivial piece of software has security vulnerabilities in it. To make matters worse, every time you click a link and every time you download an app, it is downloading more software from potentially untrusted parties and executing that too. The designers of phone operating systems have taken varying levels of precautions against these bits of code being able to steal your personal data or hijack the wireless transmitter on the device, but even the best of those precautions are themselves potentially faulty and riddled with bugs and vulnerabilities. And as bad as that sounds, the situation with phones is almost certainly better than the situation with the myriad other wireless devices in our lives: security cameras, cars, thermostats, baby monitors, door locks, and even medical and public safety equipment.

Finding these vulnerabilities takes a lot of work, and it's a cat and mouse game between the criminals and foreign governments who would exploit these vulnerabilities and the security researchers and software developers who try to find them and fix them first. Absent technological advances in software engineering, the best we can hope for is that the good guys stay ahead of the curve in this game of finding the vulnerabilities before the criminals do. But we can't stay ahead of the curve if the fixes don't get released for older devices that are still in active use by millions of Americans. It does no good for the owners of these older devices to only deliver these fixes on new devices. And it leaves our networks, filled with these old devices, vulnerable as well.

I can hear the objections. Here is yet another FCC Commissioner who's grown too big for his britches. He wants to regulate software security. Others have tried and failed. Show me, Mr. Commissioner, just where in the Communications Act does it give the FCC the authority over cybersecurity?

I hear you. But the FCC has and has always had the specific authority I'm talking about: the power to protect signal security. Title 3 of the Communications Act gives us expansive authority to regulate RF emitting devices to make sure they don't cause harmful interference. It

is with this authority that we set the parameters of spectrum licenses, that we regulate the power levels at which devices can operate, and under which we require just about every electronic device sold in America to meet our conditions and receive our imprimatur.

It is true that vulnerabilities in device software can give rise to data theft and other application-level incidents that are usually thought of as outside of the FCC's purview. But they also give rise to a more purely physical threat. A vulnerable device can be hijacked by an attacker and turned into a signal jammer. This threat is anything but theoretical. Wi-Fi deauthentication attacks, which can render useless every Wi-Fi network in an area, can be carried out by a single device with a Wi-Fi antenna. Mobile phone basebands, the components that handle LTE or 5G connectivity, can be hijacked; and research has shown that botnets consisting of compromised handsets can be used to successfully attack and degrade wireless networks across large areas. And because of the nature of computing platforms and operating systems, a vulnerability in one component of a device, which might not be directly related to wireless transmission, can be leveraged to attack other components of that device. Any vulnerability in a phone operating system, in a smart thermostat firmware, in a 5G base station, is a threat to the security of our wireless networks from harmful interference. This makes it very much the FCC's concern.

In fact, I believe that our equipment authorization and spectrum licensing regime includes such a requirement already. It's just a matter of updating our assumptions about what's possible. There's no question that if, after we'd authorized equipment, a flaw in such equipment caused it to put out large amounts of harmful interference, we would expect the manufacturer to stop selling the device and to take reasonable steps to stop the harmful interference emitting from the already-sold units. That's why there's post-market surveillance as a well-established practice already. Similarly, it would violate our rules for a manufacturer of a Wi-Fi router to put out an update that disabled dynamic frequency coordination or increased transmission power levels beyond the allowed limits. What I am saying today is not much different. If a manufacturer becomes aware of a security vulnerability in its device that might facilitate an attacker in co-opting the device into producing harmful interference, then that manufacturer needs to take reasonable steps to prevent it from happening. In most cases, the most reasonable course of action would be to issue a software or firmware update to patch the security flaw and to therefore make sure in the design phase that the equipment could be easily patched.

But I think the industry would benefit from more than just the broad reasonableness standard implicit in our current rules. This is a complex issue and there are countervailing interests as well. For one, a company should at some point be able to abandon its engineering efforts for old and obsolete product lines, even if they remain in some amount of use by the public. No one expects Ford to pay for a recall for a car they sold in 1980. I believe the FCC needs the wireless equipment industry to help us formulate rules that protect the public by raising the bar for security practices while also making sure that industry is not bogged down with perpetual legal obligations to long-abandoned product lines. I look forward to productive engagement and hopefully not knee-jerk opposition. This is an opportunity to address this emerging problem with a bipartisan, pro-innovation approach.

Security patches are not an unrealistic requirement. Thousands of software and consumer products companies have done tremendous jobs developing secure automatic update systems, which we now rely on as a matter of course for computers and phones. Even microprocessors, once the definition of locked-down, burned in systems, are now remotely patchable. But this isn't just about computers and phones. For example, the auto industry has come together in the Uptane project to develop a common framework for automatic updates. When many companies do get it right, and now that security patches are part of our daily lives, it is not credible to suggest that you should be allowed to sell a device and one or two years later abandon it and allow security vulnerabilities to fester in the pockets and homes of millions of Americans.
My door is open. We want to meet with industry, with engineers, with security researchers, with other parts of the government. Together we can transform the security of America's wireless devices and networks.

Thank you.